

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION

FINTIV, INC.,

Plaintiff,

v.

APPLE INC.,

Defendant.

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

Civil Action No.: 6:18-CV-372-ADA

JURY TRIAL DEMANDED

**DECLARATION OF DR. DON TURNBULL IN SUPPORT  
OF APPLE'S PROPOSED CLAIM CONSTRUCTIONS**

**I. INTRODUCTION**

I, Don Turnbull, declare as follows:

1. I have been retained by counsel for Apple Inc. in the above-captioned action as an independent expert consultant to offer opinions regarding how a person of ordinary skill in the art (“POSITA”) would understand certain claim terms in U.S. Patent No. 8,843,125 (“the ’125 patent”).
2. I am informed that the parties have proposed the following constructions for the claim terms listed in the table below:

<b>Claim Term</b>	<b>Apple’s Construction</b>	<b>Fintiv’s Construction</b>
“wallet management applet (WMA)” (claims 11 and 13)	“software application for storing duplicate account specific information accessible to the mobile wallet application”	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is “integrated functionality that enables management of a wallet related applet.”
“widget” (claims 11, 18, and 23)	“user interface software application”	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is “integrated functionality that relates to applications related to a financial institution transportation account, and the like.”
“mobile wallet application” (claims 11, 18, and 23)	“mobile wallet software application capable of being independently downloaded and installed”	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is “application that provides wallet functionality on the mobile device.”
“SE information” (claims 14 and 23)	“information relating to the secure element”	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is “information related to the secure element that may include at least card production life cycle, card serial number, card image number, and integrated circuit card identification.”

<b>Claim Term</b>	<b>Apple's Construction</b>	<b>Fintiv's Construction</b>
"mobile device information" (claims 14, 18, and 23)	"hardware or software properties relating to the mobile device"	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is "mobile device related information."
"over-the-air (OTA) proxy" (claim 23) and "OTA proxy" (claim 16)	"mobile device software application for communicating between a secure element and a server over a mobile network"	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is "functionality for creating a secure connection."
"provision[ing]" (claims 11 and 23)	"provid[e/ing] and/or mak[e/ing] available for use"	Plain and ordinary meaning. To the extent the Court requires construction the plain and ordinary meaning is "making available for use."

3. I have been asked to opine on how a POSITA would understand each of these terms as used in the '125 patent with the exception of the term "provision[ing]." I understand that Apple has offered to stipulate to Fintiv's proposed construction of the term "provision[ing]" and that the only remaining dispute between the parties is whether the court should construe the term.

## **II. QUALIFICATIONS**

4. I am an expert in software design and architecture, including networked and mobile systems, with over 30 years of research and development experience. My research and development endeavors cover various technologies related to information systems including information organization and retrieval; collecting, analyzing and modeling user behavior; application and interface design; and data-focused networked, mobile, and web systems for eCommerce.

5. My experience includes helping software companies, from small startups to large corporations, create new technologies and applications. To advise these companies, I research and monitor academic and industry technology developments to keep up-to-date regarding advances in the field. I am also aware of the history of software development from my professional and academic experience over the past 30 years.

6. In 1988, I graduated with a B.A. in General Studies (“Knowledge Engineering”, computer science, psychology, and philosophy/logic) from The University of Texas at Arlington. I focused on two areas of computer science at the time, Artificial Intelligence (Expert Systems) and Hypertext Systems. Following my university studies, I immediately worked in software development to create hypertext markup documents with a focus on the combination of my two areas of emphasis. In the era just before the Web, 1991-1994, I was a software engineer and software methodologist creating Macintosh, Microsoft Windows, and IBM OS/2 software for building client/server applications that worked with (relational) databases over networks, which proved to be much of the supporting technology for Internet and Web applications. This included programming and working as a database administrator and using early Internet networking tools. I also designed and built early hypertext (SGML) authoring tools, which led to a more commercial use of the Internet and also allowed me to become familiar with Web browser applications by 1993.

7. In 1995, I earned an M.S. in Information Design and Technology from the Georgia Institute of Technology where my concentration was on Internet and Web systems in their very early days including early studies of eCommerce systems where merchandise could be browsed and purchased via the Web.

8. In 1996, I was a Lead Technical Architect at IBM where I worked on building an Internet client/server platform for a multimedia client application combined with a database-driven Web site—the IBM-WorldBook Encyclopedia. I also contributed to designs and advised on numerous other ongoing Internet-focused projects at IBM, including Web site development tools for eCommerce small business Web sites, large enterprise (intranet) Web sites including portals, as well as the foundations for a Web site usability practice at IBM to evaluate Web use of IBM software and server-based applications.

9. From IBM, I went to the doctoral program at the University of Toronto where I investigated Web technologies and database technology, especially as applied to eCommerce businesses. I conducted research into large-scale digital content repositories, enterprise systems including banking data analytics, and early work into Web Data Mining and Web Analytics and data capture solutions for understanding Web use.

10. As I was completing my dissertation work in 1999 in Toronto, I joined a startup in the Bay Area that was a spin-out from Xerox PARC called Outride, where we focused on collecting and analyzing user Internet access data to provide personalized services on demand. Outride's technology was a combination of work from Xerox PARC researchers and my own to build contextual, behavioral models (what we later coined as "contextual computing") to provide personalized content based on the specific user, their environment, their device, and other characteristics. Outride was acquired by Google in 2001 and folded into their own growing personalization technology. Among the technology acquired by Google from Outride, I am the primary inventor of a patent focused on "Interface And System For Providing Persistent Contextual Relevance For Commerce Activities In A Networked Environment" (US Patent No. 7,089,237) that included functionality to provide services and content filtered to a specific user as well as to enable and enhance mobile e-commerce.

11. In 2002, I received my Ph.D. in Information Studies from the University of Toronto where my research centered on information systems with a focus on Internet-scale data collection and analysis to understand and model user behavior. My thesis was titled "Knowledge Discovery in Databases of Web Use: A Search for Informetric and Behavioral Models of Web Information Seeking."

12. From 2002-2009, I was an Assistant Professor at the School of Information at The University of Texas at Austin where I created and taught a variety of graduate-level courses including: Information Architecture and Web Design; Web Information Retrieval, Evaluation &

Design; the Semantic Web; Information System Analytics; and Web Information System Design and Knowledge Management Systems. As faculty, principal investigator, and research team director, my areas of exploration included designing information system interfaces and architectures; large-scale data mining and algorithms (including Web use data for personalization); techniques for interface design for multimedia access; mobile interaction techniques; Web content classification; and the design of Web search engines, as well as studying their use.

13. While an Assistant Professor, I formed and managed a number of research projects. These projects included information architecture and design for digital media; early mobile application design guidelines and prototypes for context-aware mobile systems; and a set of methods for content analysis and topic distillation. I also advised graduate students and coordinated information technology research and development. These included Semantic Web applications, mobile information system prototypes and server architectures, user understanding of digital content manipulation, Web accessibility evaluation, Web link mining and analysis, information architecture design methodologies, and Web advertising methods and platforms.

14. Following my full-time position at UT Austin, I worked with other departments at the University including the Institute for Innovation, Creativity and Capital (IC<sup>2</sup>) and the Austin Technology Incubator. While there, I helped mentor startups on technologies including mobile systems and eCommerce/payment systems, as well as advised the University on entrepreneurship efforts as well as intellectual property evaluation. In 2012, I began working more directly with startups in the mobile space to share my ongoing expertise, including decontextualizing games for alternate monetization processes and mobile device usage data collection for attribution tracking and compensation. In the past few years, I have also been more directly involved in mobile software development as the architect of a system to gather, process and manage mobile behavior for predicting purchase behavior including a pending patent application.

15. My other current work centers on software research and architectural design in the areas of information systems, with a focus on utilizing my research background and deep experience designing software applications to advise companies on both technical and business issues. This work includes consumer and enterprise applications such as content management systems, mobile technologies, recommendation systems, personalization, analytics applications, search tools and eCommerce platforms for mobile and Web. I am also involved in researching and architecting solutions related to data mining and data science, collecting Web and mobile usage data, information architecture and design, and general information systems design.

16. I am also the author of numerous academic publications including: a textbook on Web-based information seeking and knowledge work; articles on human-computer interaction design; personalization for Web-information-retrieval and recommender systems; and numerous definitive works on information-architecture (Web site) methodologies, designs, and implementations. In addition, I am the named inventor on at least one United States patent involving Web technologies focused on content delivery and personalization related to algorithmically providing services to a user based on contextual properties such as device and location.

17. Other details concerning my background, academic work, and professional history are set forth in my curriculum vitae, which is attached as Ex. A to this declaration.

### **III. COMPENSATION**

18. I am being compensated for my services in this matter according to my standard hourly rate for consulting services, which is \$675 per hour. My compensation is not contingent upon the opinions I render or the outcome of this litigation.

### **IV. MATERIALS CONSIDERED**

19. In preparing this declaration, I reviewed and considered the following materials, and any others referenced in the body of my declaration:

- the '125 patent and its file history;
- U.S. Pat. App. No. 61/428,846 (“‘846 provisional”);
- U.S. Pat. App. No. 61/428,851 (“‘851 provisional”);
- U.S. Pat. App. No. 61/428,852 (“‘852 provisional”);
- U.S. Pat. App. No. 61/428,853 (“‘853 provisional”);
- Apple and Fintiv’s respective opening claim construction briefs;
- All exhibits attached to Apple and Fintiv’s respective opening claim construction briefs; and
- Documents and papers cited herein including:
  - Excerpts from “How to Do Everything with Your Zire Handheld,” by Dave Johnson and Rick Brioda, published by McGraw-Hill Companies, 2003 (Ex. B hereto);
  - Excerpts from “Ilium Software eWallet Users Guide and Reference for Windows Pcs and Palm Powered handhelds,” Version 4.0, Ilium Software, Inc., 2006 (Ex. C hereto);
  - “A Personalized Offer Presentation Scheme for Retail In-Store Applications,” Liu Yew-Hyey, Jih-Shyr Yih, and Trieu C. Chieu, 2004, IBM T. J. Watson Research Center, in K. Bauknecht, M. Bichler, and B. Pröll (Eds.): E-Commerce and Web Technologies, 2004, Lecture Notes in Computer Science, vol 3182. Springer, Berlin, Heidelberg, pp. 296-304, 2004. Springer-Verlag Berlin Heidelberg (Ex. D hereto);
  - “Towards a Mobile Digital Wallet,” Alan Cole, Scott McFaddin, Chandra Narayanaswami, and Alpana Tiwari, IBM Research Report, October 16, 2009 (Ex. E hereto);
  - Excerpts from Microsoft Computer Dictionary (2002) Fifth Edition (Ex. F hereto);
  - Excerpts from Newton’s Telecom Dictionary, 24th edition, 2008 (Ex. G hereto);
  - Excerpts from 2010 New Oxford American Dictionary (Ex. H hereto);
  - Excerpts from “X Window Systems User’s Guide Volume Three,” Valeria Quercia and Tim O’Reilly, O’Reilly & Associates, Inc. Sebastopol, CA. 1990 (Ex. I hereto);
  - Gookin, Dan. 2010 - Droid X For Dummies. Wiley Publishing, Inc., Indianapolis, Indiana, 2010 (Ex. J hereto);
  - Excerpts from Microsoft Computing Dictionary 2002, Fifth Edition (Ex. K hereto);



- Excerpts from “Apache the Definitive Guide 2nd edition,” Laurie, Ben and Laurie, Peter. 2000, O’Reilly & Associates, Sebastopol, CA (Ex. L hereto).

20. I may use these documents and information, or other information obtained during the course of this or related proceedings, as well as representative charts, graphs, schematics and diagrams, animations, and models based on those documents and information, to support and to explain my opinions. I am informed that discovery in this action has not concluded and I reserve the right to modify or supplement my opinions, this declaration, and/or to submit additional declarations to address any information obtained, or positions taken.

21. My opinions are based in part on a review and analysis of the above-mentioned documents and materials. I have also drawn on my education, experience, and knowledge of basic software and hardware engineering principles, software design, computer science, and e-commerce services such as mobile payment systems comprised of mobile devices, and servers, and components thereof.

## **V. LEGAL STANDARD**

22. I am not a legal expert or an attorney, and offer no opinions on the law. I understand that claim construction is a matter of law. However, I have been informed by counsel of the legal standards that apply to claim construction, and I have applied them in forming my opinions.

23. I have been informed that the words of a claim are generally given the ordinary and customary meaning that the term or phrase would have to a POSITA at the time of the invention in view of the surrounding claim language, the specification and the file history (collectively, the “intrinsic evidence”). I also understand that courts may consider extrinsic evidence, such as expert and inventor testimony, dictionaries, and learned treatises, but that such extrinsic evidence should be given less weight than the intrinsic evidence.

24. I have been informed that provisional applications incorporated by reference in a patent specification are considered part of the specification as if fully set forth therein and are just as relevant to claim construction as the rest of the specification.

25. I have been informed that a term must be interpreted with a full understanding of what the inventors actually invented and intended to include within the scope of the claim as set forth in the patent itself. Thus, claim terms should not be broadly construed to encompass subject matter that is technically within the broadest reading of the term but is not supported when the claims are viewed in light of the invention described in the specification. I have also been informed that when a patent specification repeatedly and consistently characterizes the claimed invention in a particular way, it is proper to construe the relevant claim terms in accordance with that characterization.

#### **VI. LEVEL OF SKILL IN THE ART**

26. I am informed that Fintiv asserts that the priority date for the '125 patent is December 30, 2010. I have been instructed by counsel for Apple to use that priority date in forming all of my opinions herein and have done so. I understand that factors such as the education level of those working in the field, the sophistication of the technology, the types of problems encountered in the art, the prior art solutions to those problems, and the speed at which innovations are made may help establish the level of skill in the art.

27. I find the pertinent art for the '125 patent to lie generally in the field of information systems and software engineering. Based on my review of the technology, the educational level of active workers in the field, and drawing on my own experience in the field, it is my opinion that a POSITA in the timeframe of Fintiv's alleged December 30, 2010 priority date would have had a degree in Computer Engineering, Computer Science, Information Systems, or in a similar discipline, and have 3-4 years of experience with the design and/or implementation of mobile

applications in a client/server environment using mobile application development platforms, APIs, and protocols. A relevant graduate degree may substitute for some work experience.

28. At all relevant times, I have exceeded the qualifications of a POSITA and managed many persons who met or exceeded this education and experience level. By December 2010 I had already earned my doctorate degree and had been teaching graduate-level courses on the pertinent technologies at the University of Texas at Austin for over 7 years with students that met my definition of a POSITA. By this time, I had also designed and developed mobile applications that built upon my extensive background as a software developer, for example having been a Java developer provided insights into programming for Google's Android mobile platform. Additionally, my experience as a NeXTStep and MacintoshOS developer provided a foundation for understanding Apple's iOS mobile platform. Notwithstanding that I exceeded the qualifications of a POSITA, I have formed my opinions from the perspective of a POSITA.

## **VII. TECHNOLOGY BACKGROUND**

29. The technology of the '125 patent relates to software running on a mobile device, and related server-side software, for storing, managing, and administering e-Commerce applications and data in a metaphorical "mobile wallet." By December 2010, there was already a robust ecosystem of popular mobile "smartphone" devices, including those running at least Google's Android mobile operating system and Apple's iOS mobile operating system.

30. Naturally, there was a rich history of prior mobile devices, mobile operating systems, commerce or wallet-like data management applications, as well as the supporting infrastructure such as servers, synchronization functionality, applications, and interfaces to provide commerce tools "on the go" with mobile devices. As early as the 1980's there were financial management applications for personal computers that provided singular management of financial data that included creating, storing, updating, syncing and backing-up commerce and financial data such as credit card or banking information. In this early personal computing era, there was a

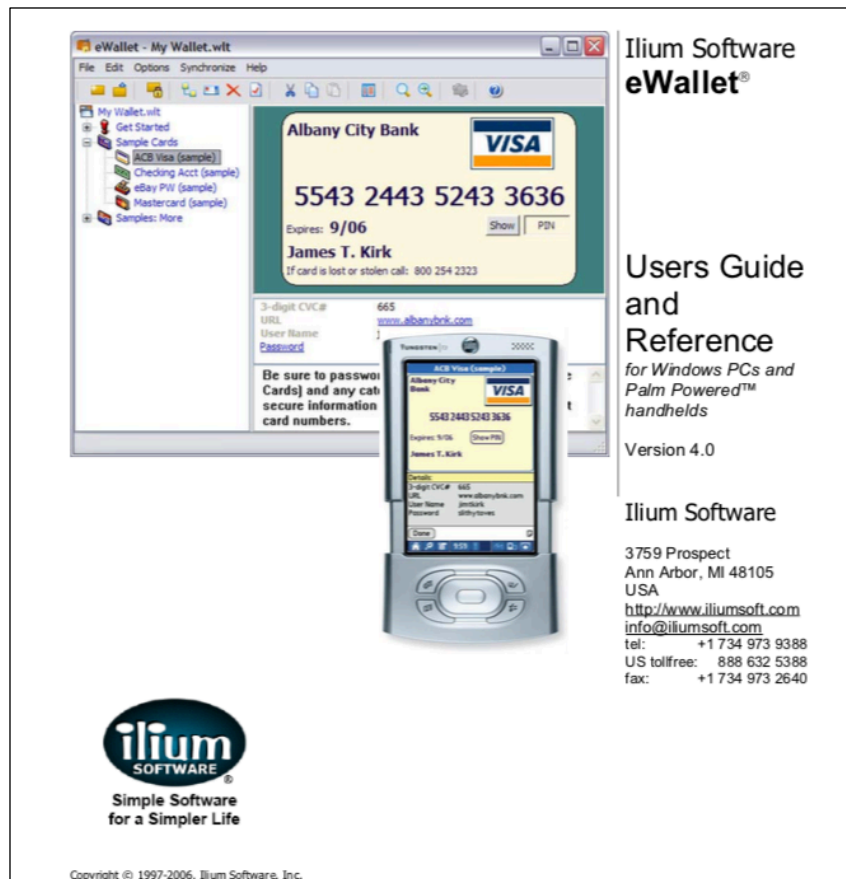
proliferation of what were called “personal information management” applications, that allowed secure storage of personal information on the computer, which could include all manner of financial information such as credit card numbers or banking data. As personal computing technology became smaller and more portable, this concept evolved into the Personal Digital Assistant (or “PDA”), a term made popular by the Palm Pilot mobile device in the mid-to-late 1990’s. The Palm Pilot included its own applications for personal information notes and also provided syncing between the mobile PDA and a desktop server. These Palm devices also could connect to the Internet and perform basic, early smartphone functionality like email and Web browsing. The Palm Pilot’s Palm OS also allowed for installation of third-party applications, one being the *ExpensePlus* application by WalletWare, as shown in the screenshot below.



Ex. B (“How to Do Everything with Your Zire Handheld,” by Dave Johnson and Rick Brioda, published by McGraw-Hill Companies, 2003, page 140).

31. The WalletWare application helped to manage expenses and receipts including personal financial information and could be synced to the user’s desktop computer and even be integrated with expense forms in other desktop applications like Microsoft Excel. *Id.*

32. In 1997, these mobile wallet ideas were built on by Ilium Software's eWallet application for the Palm (as well as for the Microsoft Windows Mobile platform as early as 2003), which allowed for secure storage of credit card information and an expansive set of other financial information which could also be synced with a desktop system. Ilium's product documentation, such as the user guide excerpt below, shows part of their eWallet functionality.



Ex. C (Ilium Software, Inc. 1997-2006. Ilium Software eWallet Users Guide and Reference for Windows PCs and Palm Powered handhelds. Version 4.0. page 1). Like other eWallet applications, the Ilium eWallet was a software application that a user could download and install on a personal device running a compatible operating system.

33. By the mid-2000s, mobile computing devices became more common. For example, the Windows Mobile (PocketPC or Windows CE) devices were released and the aforementioned

Palm Computing Palm Pilots further developed. There was significant development that led to later smartphone mobile devices and grew into more sophisticated uses including more advanced ePayment and eWallet applications and functionality.

34. As early as 2004, IBM began building, experimenting, and releasing publications and prototype systems. One IBM publication from 2004 teaches a “rule engine” for in-store retail applications on mobile devices, including a set of “access rules.” Ex. D (“A Personalized Offer Presentation Scheme for Retail In-Store Applications,” Liu Yew-Hyey, Jih-Shyr Yih, and Trieu C. Chieu, 2004, IBM T. J. Watson Research Center, in K. Bauknecht, M. Bichler, and B. Pröll (Eds.): E-Commerce and Web Technologies, 2004, Lecture Notes in Computer Science, vol 3182. Springer, Berlin, Heidelberg, pp. 296-304, 2004. Springer-Verlag Berlin Heidelberg).

35. IBM also published another paper in 2009 describing a “Mobile Digital Wallet” specifically for the Android mobile operating system. Ex. E (“Towards a Mobile Digital Wallet,” Alan Cole, Scott McFaddin, Chandra Narayanaswami, and Alpana Tiwari, IBM Research Report, October 16, 2009). The “IBM Digital Wallet” application (shown below) described in the 2009 IBM article included security mechanisms such as access control, and wallet management including event notifications, as shown below.



36. Motorola, a well-known name in mobile technology for decades (beginning with radios, then early cell phones, and later in time more sophisticated smartphones) was researching, designing, building, and selling sale mobile technology including networking equipment, mobile devices, and mobile device applications, long before the priority date of the '125 patent. Notable devices include the ROKR smartphone, which was released in 2005. The ROKR allowed for network synchronization with third-party servers and services such as Apple's iTunes music library. Continuing through at least 2010, Motorola released a number of smartphones running various mobile operating systems from Nokia, Microsoft, and Google (Android).

37. The companies mentioned herein – Palm, Microsoft, Apple, Google, Motorola and IBM – were all, at one time or another leading up to 2010, marketplace competitors and/or technological contributors in the area of mobile PDAs, smartphones, and related software solutions.

38. As the mobile computing marketplace grew, there became a need for an easy distribution of applications for the mobile systems. Stores for mobile applications were developed as early as 1999, such as the Handango online store that sold mobile applications for Palm Pilot, other PDAs, and smartphones including Windows Mobile devices and Blackberry smartphones. By

2008, two app stores on the market were the Apple iTunes App Store (later the Apple App Store) and the Google Marketplace (later Google Play Store). These stores provided a customized experience based on the type of mobile device.

39. The Apple App Store filtered applications in the application marketplace in a number of ways. For example, it filtered apps by popularity (*e.g.*, the Top 25 apps), or using criteria like the user's past app purchase history, or rules about availability based on a particular locale. This end-user customization thus could be based on sets of broad trends and defaults, but also customized to match rules or settings specific to the user. The App Store could also identify the applications installed on a particular Apple mobile device model, and based on that information could filter what software applications were provided to a device. The App Store also provided software updates for download to the mobile device based on a variety of criteria.

40. One simple example is that a user could "upgrade" their iPhone operating system, an option which would only be shown if they were running an older version of iOS. If the iOS version was already current, no update would be provided. Another example was filtering the applications available for download or update based on the device type (iPod, iPad, iPod Touch vs iPhone).

41. The Android Marketplace (later the Google Play Store) worked in much the same manner, with a secure connection to the application server hosting a database of applications and providing only the relevant applications for the type of mobile device, the version of the Android OS and other device characteristics (*e.g.*, display resolution).

42. Thus, by 2010, there was already significant development in the technologies associated with the '125 patent, including publications, research, and actual products and systems for sale.

43. Mobile software applications were used to store and organize user card information, such as information relating to credit cards, ePayment cards, or reward cards that were stored in eWallets or other secure information storage applications. And with the advent of mobile



devices working with other computers, there was continuous development in synchronization technology, including syncing information between desktop computers and a networked server, between a mobile computing device and a networked server or in combination as applicable. The information that has long been synchronized between computers includes virtually any kind of information, from photos, email messages, and of course “cards” that could be stored in an eWallet application.

44. If requested, I am prepared to explain at a technology tutorial or claim construction hearing the technology disclosed in the ’125 patent, including the state of the art around the filing date of this patent. This may include, among other things, background information on mobile payments technology, including the components, devices, servers, and software associated with enabling mobile payments. It may also include the use of visual aids or other demonstrations.

45. I am also prepared to rebut, as necessary, matters raised by Fintiv – whether in declarations, reports, depositions, or hearings – and to address related matters raised in the course of claim construction.

#### **VIII. SUMMARY OF THE ’125 PATENT**

46. The ’125 patent discusses a wallet management system that includes mobile devices as well as servers, including certain software capabilities on each. For example, each of Figures 1 through 5 in the patent illustrate a mobile device and one or more servers in communication with each other. This is also reflected in the claims of the ’125 patent. Independent claim 11, for example, focuses primarily on the mobile device (“A method for provisioning a contactless card applet in a mobile device...”). And independent claim 18 focuses primarily on the “wallet management system (WMS)” located on the server-side. In the following paragraphs, I discuss in summary form the main aspects of the device-side and server-side components. But before

doing so, I spend a few moments discussing the two main alleged shortcomings in the prior art that the patent identifies.

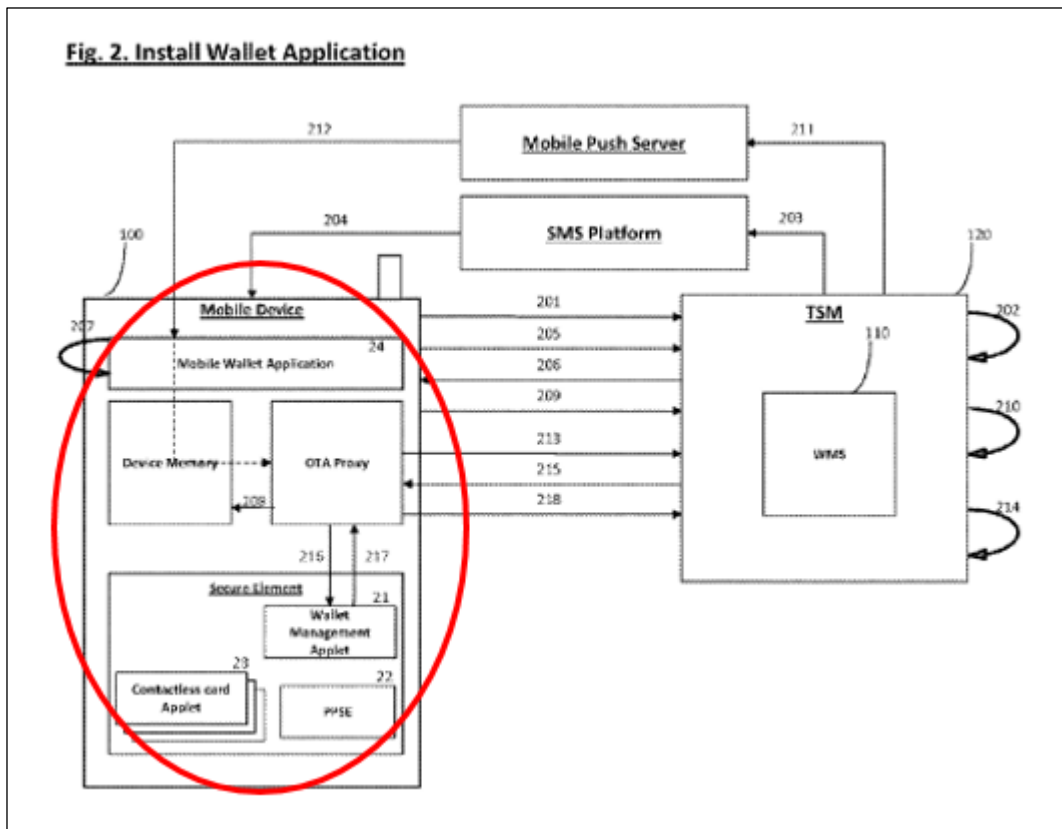
47. The first problem was that users were “often be bombarded with various [mobile wallet] applications that may be inapplicable to the user.” ’125 patent, col. 2:42-44. According to the patent, this occurred because there was a “lack of standardization of hardware and software on mobile devices.” *Id.*, col. 10:48-49. As a result, applications were “offered to the users without regard to the mobile device capabilities.” *Id.* col. 2:34-36.

48. The second major problem was that users had limited visibility and access into their own account information stored in the mobile device. The patent states, for example, that “the user may be unable to view the details related to the contactless payment applets (e.g., account number, expiration date, security code, balance and the like).” *Id.*, col. 2:13-15; *see also id.*, col. 2:27-28.

49. I also note that much of the patent’s discussion of software appears oriented towards Google’s Android operating system platform. The patent refers to technical functionality commonly used in conjunction with Google’s Android OS at the time of the alleged priority date (December 2010), such as “applet” (a Java application) or “NFC” (near field communication). Other functionality referenced in the patent, such as “Cloud to Device Messaging (C2DM)” is directly and exclusively for the Google platform. The C2DM functionality describes specific client/server applications, an application programming interface and modes of operating for the Google/Android ecosystem only.

#### **A. Components on the Mobile Device.**

50. The most detailed illustration of the mobile device components is found in Figure 2 of the patent (pasted below for reference, with red annotation identifying the mobile device which contains the components discussed in this section).



51. The patent explains that the “secure element,” (abbreviated as “SE”) “may be a smart card chip capable of storing multiple applications, including of account specific information that may not be easily accessed by external parties.” ’125 patent, col. 1:40-43. The SE is typically a chip on the mobile device where information is intended to be securely stored. Various software modules are shown in Figure 2 as being stored in the SE, including “contactless card applets” 28.

52. The contactless card applets (“CCAs”) each correspond to a physical credit or bank card found in a traditional wallet or purse. For instance, a Visa CCA corresponds to a Visa credit card. *Id.*, col. 8:61-62. Given that the CCAs store confidential information like credit card account numbers, they are located within the secure element. *Id.*, col. 8:23-28. The CCA is a considered a “contactless” applet because it uses a wireless protocol called near field communication (“NFC”) to “make payments to another NFC-compatible device by coming near

within a few centimeters of one another without physically contacting each other.” *Id.*, col. 1:54-62. The patent acknowledges that NFC technology already existed in 2010. *Id.*, col. 1:47-62.

53. As also shown in Figure 2, a so-called “wallet management applet” or “WMA” is located within the secure element. The WMA is said to be central to solving the alleged problem of user inaccessibility to their credit card information. *Id.*, col. 2:13-15 (“the user may be unable to view the details related to the contactless payment applets (e.g., account number, expiration date, security code, balance and the like)”; *see also id.*, col. 2:23-28 (“the user may be unable to view any account specific information stored within the SE”). For each CCA, according to the ’125 patent, there exists a corresponding WMA which stores a duplicate copy of the same “account specific” information found in the CCA. *Id.*, col. 8:66-9:5. It is this duplicate account information in the WMA that, together with a “widget,” enables the user to access their account information. *Id.*

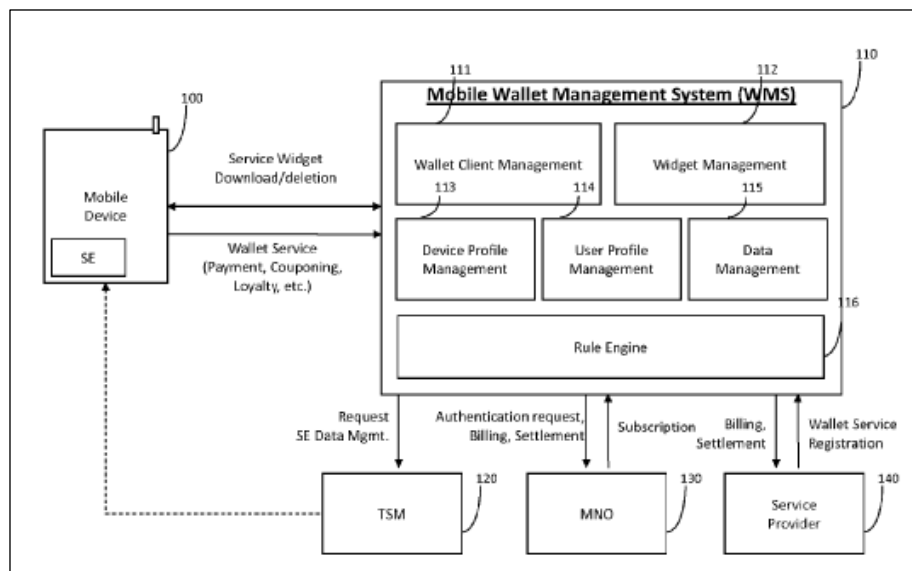
54. The aforementioned “widget” is a user interface software application that, when installed in a mobile wallet application, provides the user-facing mechanism by which the user can access his or her account information that is stored in the WMA within the secure element. *See id.*, col. 5:4-9 (“Widgets may be an application configured to interface with a user of the mobile device.”); 9:2-5 (“By installing both the WMA 21 applet and the widget, the user may view and manage the information stored in the WMA21 applet through the corresponding widget.”). Although not illustrated in the ’125 patent figures, the widget “reside[s] within the mobile wallet application.” *Id.*, col. 6:2-4.

55. Last, but not least, is the “mobile wallet application” 24. From a conceptual standpoint, the mobile wallet “may have the same composition as a conventional wallet, which may contain payment cards, member cards, transportation cards, and loyalty cards.” *Id.*, col. 1:43-46. As with the eWallets I discussed earlier, the mobile wallet application 24 in the patent is a software application that can be downloaded and installed on the mobile device, provided that it is

compatible with the operating system on the mobile device. *Id.*, col. 6:34-49; '853 provisional, Business Requirements at pages 6 and 30. Because the WMS server that I discuss in the following section stores various mobile wallet applications from different providers, users can pick which mobile wallet application they would like to download and install. *See, e.g., id.*, col. 4:61-67. The ability to install a mobile wallet is reflected in claim 1, which is directed to “[a] method for installing a wallet application.” *See also* '851, Requirements Use Cases at page 41 (“The system shall check what...wallet has been used (either SK C&C wallet or the third-party wallet.)”).

#### **B. Components on the Server-Side.**

56. Figure 1 of the patent (pasted below) provides the clearest depiction of the various aspects of the “mobile wallet management system (WMS)” (labelled 110) on the server-side. Although only six components are illustrated as being located within WMS 110, the patent says that “[t]he illustrated components may be included within the WMS 110 or external to the WMS 110.” '125 patent, col. 5:26-27. It is also important to note that patent explains that “[t]he disclosed WMS 110 may reside within TSM system 120 or independent of the TSM system 120. For the purposes of this disclosure, it will be assumed that the WMS 110 is housed within the TSM system 120.” *Id.*, col. 5:28-31. In other words, the patent says the TSM (which is an acronym for “Trusted Service Manager”) encompasses the WMS, including the modules labelled 111 through 116.



57. The patent says that the WMS was intended to address the problem users faced of being “bombarded with various [mobile wallet] applications that may be inapplicable to the user.” *Id.*, col. 2:42-44; *see also id.*, col. 10:48-49 and 2:34-36. As I previously noted, by 2010 there were a variety of mobile device manufacturers and smartphones were available on the market that had differing hardware capabilities and software configurations (*e.g.*, different operating systems and even different versions of the same operating system). The patent also explains that “business compatibility” issues (*e.g.* bank affiliation) also contributed to the problem of users being “bombarded” with “inapplicable” applications. *Id.*, col. 2:36-37.

58. To solve this problem of receiving useless or incompatible mobile applications, the patent says that the WMS “dynamically filter[s] the list of available applications based upon the mobile device attributes” and only provides compatible applications to the mobile device. *Id.*, col. 10:42-44. Thus, for example, the WMS would offer an Android device only those applications which would work on an Android device. Likewise, the WMS would send a Blackberry device only the applications compatible with it. This is consistent the discussion of various mobile device OS platform listed on page 6 of the “Business Requirements” document in the ’853 provisional application.

59. Each of the server-side components shown in Figure 1 of the patent is responsible for administering a different aspect of deploying and managing the mobile wallet software for the various mobile devices, in service of solving the incompatible app problem.

60. I begin with wallet client management component 111 which, the patent explains, is responsible for managing “the [mobile] wallet application itself.” ’125 patent, col. 4:57-5:3. The mobile wallet application is a software application that can be downloaded and installed onto a mobile device such as a smartphone. The wallet client management component 111 acts like a warehouse and stores the mobile wallet applications themselves, “including the type of wallet application and manufacturer,” because the wallet software could be provided from a variety of different manufacturers or software developers. *Id.* In this respect, the wallet client management component 111 is similar to the app stores I described in the Technology Background section. The patent refers to, for example, a mobile wallet application developed by SK C&C (*see* ’851 provisional, ¶84), a “mobile wallet application manufactured by Google®” (*see* ’125 patent, col. 4:64-67 of the ’125 patent), as well as other third-party mobile wallet applications (*see* ’851 provisional, Requirements Use Cases at p. 41).

61. WMS component 112 is the “widget management component.” This component, the patent explains, “is responsible for the individual widgets.” ’125 patent, col. 5:4-9. The term “widget,” as noted, refers to is a user interface software application that is “configured to interface with a user of the mobile device.” *Id.*

62. WMS component 113 is the “device profile management component.” According to the patent, this component “store[s] device specific information, such as information related to the mobile device itself including type of mobile device, supporting operating system (OS), mobile service provider, and other relevant information.” *Id.*, col. 5:9-16. This helps solve the incompatible app problem by providing the necessary information to filter the applications for compatibility with particular device criteria.

63. WMS component 114 is the “user profile management component.” The patent states that this component “captures user identifying information such as name, address, birthday, phone number, and the like.” *Id.*, col. 5:17-18. In a similar fashion to the device profile management component, user profile management component 114 provides input data that can be used to filter for compatible apps based on things like which bank the user has an account with.

64. WMS component 115 is the “data management component.” This component, the patent states, “allows further expansion of data management services offered by a mobile WMS (e.g., transaction history, user preferences, loyalty programs, digital receipts, digital coupons and the like).” *Id.*, col. 5:19-22.

65. WMS component 116 is a “rule engine.” This component is responsible for performing filtering “based on information related to the mobile device” which can be found in the device profile management component 113. *Id.*, col. 5:22-24. When the patent speaks of “filtering,” it means that server provides to the mobile device a “filter[ed] list of mobile widget applications that are available for installation based upon corresponding mobile device attributes,” such as the mobile device’s manufacturer or operating system. *Id.*, col. 10:9-34. Filtering is crucial to the patent because it solves the stated prior art problem that “many competing service providers” offered their services to users “without regard to the mobile device capabilities or mobile service providers utilized by the user.” *Id.*, col. 2:30-36.

66. The trusted service manager (TSM) acts as “an integration point for all of the external parties the mobile device may deal with, providing for a seamless and more efficient operation of mobile services.” *Id.*, col. 5:39-46. The TSM serves as a single point of contact for mobile devices to interact with various entities such as network providers, financial institutions, and mobile device manufacturers. *Id.*, col. 10:25-34. The TSM stores “information from various parties” and enables mobile devices to “interact with the TSM system individually rather than



various discrete entities.” *Id.*, col. 5:39-42. The patent states that “[t]he disclosed WMS 110 may reside within TSM system 120 or independent of the TSM system 120. For the purposes of this disclosure, it will be assumed that the WMS 110 is housed within the TSM system 120.” *Id.* col. 5:24-31. Accordingly, sometimes in this declaration, I use the terms TSM and WMS interchangeably.

## **IX. INTERPRETATION OF THE CLAIM TERMS**

### **A. “Wallet Management Applet (WMA)” (claims 11 and 13)**

67. Neither the term “wallet management applet” nor the acronym WMA are terms of art that a POSITA would have been generally familiar with circa 2010. A POSITA in 2010 would not have known that the acronym WMA, if used at that time, stood for “wallet management applet.” Even today, outside the context of the ’125 patent, a POSITA would not know that WMA stood for “wallet management applet.” Nor do I believe that other POSITAs would have known that WMA stood for “wallet management applet” or known what a wallet management applet was outside the context of the ’125 patent. If these terms were used at all in the 2010 timeframe, they were used sparingly and certainly did not have an established plain and ordinary meaning to a POSITA.

68. From 2002-2009, I was an Assistant Professor at the School of Information at The University of Texas at Austin, where I created and taught a variety of graduate-level courses including: Information Architecture and Web Design; Web Information Retrieval, Evaluation & Design; the Semantic Web; Information System Analytics; and Web Information System Design and Knowledge Management Systems. In none of these courses did I use the term “wallet management applet” or “WMA” and those terms do not appear in the course materials I used or any popular references such as computing dictionaries or programming guides, nor any academic textbooks or research papers.

69. In fact, in the 2010 timeframe, WMA would have at best been known as the file extension for a Windows Media Audio file (a “.wma file”). *See* Ex. F (Microsoft Computer Dictionary (2002) Fifth Edition, pages 570 and 573).

70. That said, the singular term “applet,” by itself, had a plain and ordinary meaning to a POSITA in 2010. By far, the most widely understood meaning of the term “applet” was in the context of Java, although applets could also be written in other programming languages. Java applets were part of the open, object-oriented programming language and platform developed by Sun Microsystems in the early 1990’s. The Java language, and its accompanying services platform for network-enabled applications of all manner, became one of the most popular programming languages and platforms as early as 1996, continuing to today. As noted earlier, the Java programming language was and is still the primary programming language used to build mobile applications and data management frameworks for Google’s Android operating system. At the time of the invention, it was not possible to use or run native Java applications or applets on an Apple mobile device.

71. I was an early adopter of the Java programming language, which I used as early as 1994 while at Georgia Tech to build and experiment with small multimedia applications that ran inside a Java or Java-capable Web browser by building simple applets in Java that would, for example, play interactive audio or video. I had prototyped Android apps in Java as well, as early as 2009, and often permitted and referenced Java development in my graduate courses at UT Austin.

72. The meaning of “applet” is reflected in numerous technical materials, such as Newton’s Telecom Dictionary, 24<sup>th</sup> edition, which was published in 2008 and defines “applet” as a “mini-program[] that can be downloaded quickly and used by any computer with a Java-capable browser.” Ex. G.

73. The familiarity a POSITA would have had with the term “applet” does not mean, however, that the longer phrase “wallet management applet” had a plain and ordinary meaning. As I stated before, it did not.

74. A POSITA would, however, have understood the term WMA upon reviewing the intrinsic evidence of the ’125 patent. A POSITA reading the ’125 patent specification, including the provisional applications, would understand the term wallet management applet to be a software application for storing duplicate account specific information accessible to the mobile wallet application. The term WMA is used over 100 times in this way throughout the combined specification of the ’125 patent. Consistent with a POSITA’s understanding of the term “applet” described above, the ’125 patent consistently uses the term WMA to refer to a software application. For example, the ’846 provisional says that “[the WMA] is a software application [residing] within the secure element of the mobile device which stores account specific information such as a credit card number.” ’846, ¶42. The glossary near the end of the ’851 provisional states that an applet is a “[r]epresentation of a chip application software and/or data” and that “[i]n this document, it refers to an application on a Java card.” ’851, Requirements Use Cases at page 50. This further confirms that a POSITA would understand the WMA to be a software application.

75. The ’125 patent also says that “[t]he WMA 21 container is a software application ...” ’125 patent, col. 7:16-19. Further confirmation exists in numerous places where the claims and combined specification talk about “downloading” and “installing” the WMA. For instance, claim 16 states “transmitting a request for installation of the contactless applet and the corresponding widget and WMA to be installed.” *See also, e.g.*, ’851 provisional, Software Requirements, p. 32 (“Wallet system acknowledges to wallet application to download WMA...After acknowledge of completion of WMA installation from the OTA proxy”); ’853 provisional, Business Requirements, p. 11 (“In order to launch the mobile wallet service, the

Wallet Client shall first be activated. During the activation process, the WMA may be downloaded and installed in the SE and it will need to be integrated with TSM for information registration.”).

76. The specification, including the four provisional applications, also makes clear to a POSITA that the WMA stores duplicate account specific information. Indeed, that is the essential purpose of the WMA. As the ’846 provisional says: “The WMA 21 is a software application to reside within the within the secure element of the mobile device which stores account specific information such as a credit card number. WMA 21 is unique in that its primary purpose is to cause contactless card applet 23 account information to be stored within the mobile device’s SE separate from the contactless card applets 23. As the issuers of contactless card applets 23 do not allow direct access into the applets themselves, duplicate account information may be stored separately within the WMA 21 in order for the mobile wallet application to view account specific information (e.g. credit card number, security code, PIN, expiration date, and etc.)” ’846 provisional, ¶42. The ability to store a copy of a user’s account information and make it accessible to the user via the mobile wallet application is what sets the wallet management applet apart from other types of applets. This same concept is repeated many, many times throughout the combined specification, including in each provisional application. For instance, the ’851 provisional contends that because “mobile devices cannot access the payment applets directly, a separate WMA 501 is required” and that “WMA 501 will store duplicate payment applet account information so that mobile wallet application may access the account specific information stored within the SE.” ’851, ¶¶89-90. The ’852 provisional reiterates that “duplicate financial information is created ... and sent to be provisioned into the WMA.” ’852, ¶¶76-77; see also *id.*, ¶62. And the ’853 provisional says that a “separate WMA 501 is required for the management of mobile wallet cards stored within mobile wallet application. During the provisioning process, WMA will store duplicate account information as

the payment applet, so that mobile wallet application may access the account specific information stored within the SE.” ’853, ¶78. And the ’125 patent specification says that “account specific information is installed into WMA 21...” (’125 patent, col. 9:45-48) and that “[t]he respective account information or WMA 21 applet may be provided by duplicating the account information associated with the contactless card” (*id.*, col. 7:43-47). The consistently repeated message is that the defining characteristic that makes the WMA “unique,” is that it stores a copy of the CCA account specific information “separate from” the CCA.

77. This is reinforced by the ’125 patent’s explanation that users of prior art mobile wallets could not access their account information when it was stored in a CCA. As stated in the ’846 provisional, the contactless card applets “do not allow direct access into the applets themselves.” ’846, ¶42. There was, according the patent, no way for the mobile wallet application (or by extension the user) to “view account specific information” stored in the CCA, such as the “credit card number, security code, PIN, [and] expiration date.” *Id.*; *see also* ’125 patent, col. 7:32-37. The patent’s solution was to store “duplicat[e] account information” in the WMA that could be accessed via the mobile wallet application. *Id.*, 7:43-47; *see also, e.g.*, ’851 provisional, ¶90 (“During the provisioning process, WMA 501 will store duplicate payment applet account information so that mobile wallet application may access the account specific information stored within the SE”); ’846 provisional, ¶42 (“As the issuers of contactless card applets 23 do not allow direct access into the applets themselves, duplicate account information may be stored separately within the WMA 21 in order for the mobile wallet application to view account specific information (e.g. credit card number, security code, PIN, expiration date, and etc.).”); ’853 provisional, ¶78 (the WMA stores duplicate account information “so that mobile wallet application may access the account specific information stored within the SE”).

78. The patent says that users were “unable to view the details” of the CCAs, such as their account specific information. ’125 patent, col. 2:8-15. Consequently, users were said to be

“unable to effectively manage or keep track of various contactless payment applets stored in their respective mobile devices.” *Id.*, col. 2:16-18. Only if the account information was duplicated in the WMA could the mobile device, via the wallet application, “access the information.” *Id.*, col. 9:45-48; *see also* ’851 provisional, ¶89 (“as mobile devices cannot access the payment applets directly, a separate WMA 501 is required for the management of mobile wallet cards stored within mobile wallet application”); ’853 provisional, ¶78; ’846 provisional, ¶59

79. In summary, my opinion is that a POSITA would understand the term “wallet management applet (WMA)” in the ’125 patent to mean a software application for storing duplicate account specific information accessible to the mobile wallet application.

**B. “Widget” (claims 11, 18, and 23)**

80. A POSITA at the time of the ’125 patent’s alleged priority date would have understood that the term “widget” is a technical term that is used in the ’125 patent in a manner that differs from its ordinary usage outside of the technical context of the ’125 patent as a generic name for an object or device that has no particular description.

81. In view of the intrinsic evidence, a POSITA at the time of the ’125 patent’s alleged priority date would have understood “widget” to refer to a “user interface software application.”

82. A POSITA would have come to this understanding based on the ’125 patent’s explanation of the objectives of the patent’s purported invention and the consistent and repeated usage and discussion of widgets as user interface software applications.

83. As I explained in the Summary of the ’125 Patent section above, the ’125 patent purports to have solved the problem that prior art mobile wallets did not allow the user to “view the details related to the contactless payment applets (e.g., account number, expiration date, security code, balance and the like).” *See* ’125 patent, col. 2:13-15; *see also id.*, col. 2:27-28. The ’125 patent describes only one user interface component that could allow the user to view this information, and it is a widget in the form of a software application, as I explain in the following

paragraphs. Thus, a POSITA reading the '125 patent would have understood that a user interface software application would have been necessary, in the context of the '125 patent, in order to solve this stated problem in the prior art.

84. The '125 patent consistently refers to widgets as “user interface software applications.” For example, claim 11 is a “method for provisioning a contactless card applet in a mobile device” in which the mobile device connects to a TSM and, after the user selects a CCA, the mobile device “retriev[es] a widget...corresponding to the [CCA]” and “provision[s] the selected [CCA and] the widget,” and the server of claim 18 includes a widget management component that stores widgets for downloading. A POSITA would understand these claims to be referring to a widget application that is downloaded from the server to the mobile device for provisioning.

85. And the specification states, for example, that widgets are user interface “applications stored at the application level related to a financial institution, transportation account, and the like.” *See* '125 patent, col. 4:57-61; *see also id.*, col. 5:6-9 (“Widgets may be an application configured to interface with a user of the mobile device. In an example, widgets may refer to individual payment applications, transportation applications, and other related applications”); 5:66-6:4 (the widget may reside “within the mobile wallet application”). This meaning is used countless more times throughout the '125 patent specification. *See, e.g.*, '125 patent, col. 2:13-19, 4:5-9, 8:19-22, 10:10-14, 8:60-9:5.

86. Similarly, in the four provisional applications that the '125 patent states are incorporated into the specification by reference, the widget is again consistently described as a user interface software application or using similar language which a POSITA would understand to refer to a user interface software application. *See, e.g.*, '851 provisional, Requirements Use Cases document at pp. 18-19, 44 (the widget is a “widget binary file”); '853 provisional, Business Requirements document at p. 30 (the widget is a “downloadable sub module of a wallet client,” and the wallet client is a “downloaded mobile application”); '846 provisional, ¶53 (“when a

request to provision the selected [CCA] is made, a corresponding...widget (user display for the contactless card application 23 stored in the WMA 21) [is] also requested to be provisioned automatically”);’846 provisional, ¶30 (“[w]idgets represent individual payment applications, transportation applications, and other related applications”); ’852 provisional, ¶77 (“widget application will be installed in the SK C&C wallet for graphic display of the installed account”).

87. In light this of this repeated and extensive discussion, a POSITA would have understood that the widget claimed in the ’125 patent is a user interface software application.

88. I observe that this understanding is also confirmed by contemporaneous extrinsic evidence. For example, the definition of “widget” in the 2010 New Oxford American Dictionary for the computing field is “an application, or a component of an interface, that enables a user to perform a function or access a service.” Ex. H. One of the earlier uses of the term widget in software engineering goes back to at least 1990, where widgets were part of the X Window System, a network-based graphics windowing system for UNIX workstations, and defined as “pre-defined user interface components or objects.” Ex. I (Quercia, Valerie and O’Reilly, Tim. 1990. X Window Systems User’s Guide Volume Three, O’Reilly & Associates, Inc. Sebastopol, CA. Page 15). This general reference to an interface element in a particular style was commonplace and only changed over time to match the capabilities or the limitations of new or particular operating systems and programming frameworks going forward. Indeed, in 2010, a widget in the Android operating system environment was described as “a teensy program that can display information, let you control the phone, access features, or do something purely amusing.” Ex. J (Gookin, Dan. 2010 - Droid X For Dummies. Wiley Publishing, Inc., Indianapolis, Indiana. Page 43).

89. In summary, it is my opinion is that a POSITA would understand the term “widget” in the ’125 patent to be a user interface software application.



**C. “Mobile Wallet Application” (claims 11, 18, and 23)**

90. In the past decade, mobile devices and “apps” or “applications” have become more and more common. Thus, today, even lay persons may be familiar with what is meant by the general term “mobile app” or “mobile application.” Nevertheless, the claim phrase “mobile wallet application” is less well-known among the general population and remains at least somewhat of a technical term. Moreover, at the time of the alleged priority date in 2010, it was an even more obscure and technical term because mobile applications generally, and mobile wallet applications in particular, had yet to find their way into the mainstream.

91. A POSITA at the time of the ’125 patent’s alleged priority date, especially in view of the intrinsic evidence, would have understood that a mobile wallet application referred to a mobile wallet software application capable of being independently downloaded and installed onto a mobile device.

92. A POSITA would have come to this understanding based on the ’125 patent’s explanation of the objectives of the patent’s purported invention and the consistent and repeated usage and discussion of mobile wallet applications as software applications capable of being independently downloaded and installed onto a mobile device.

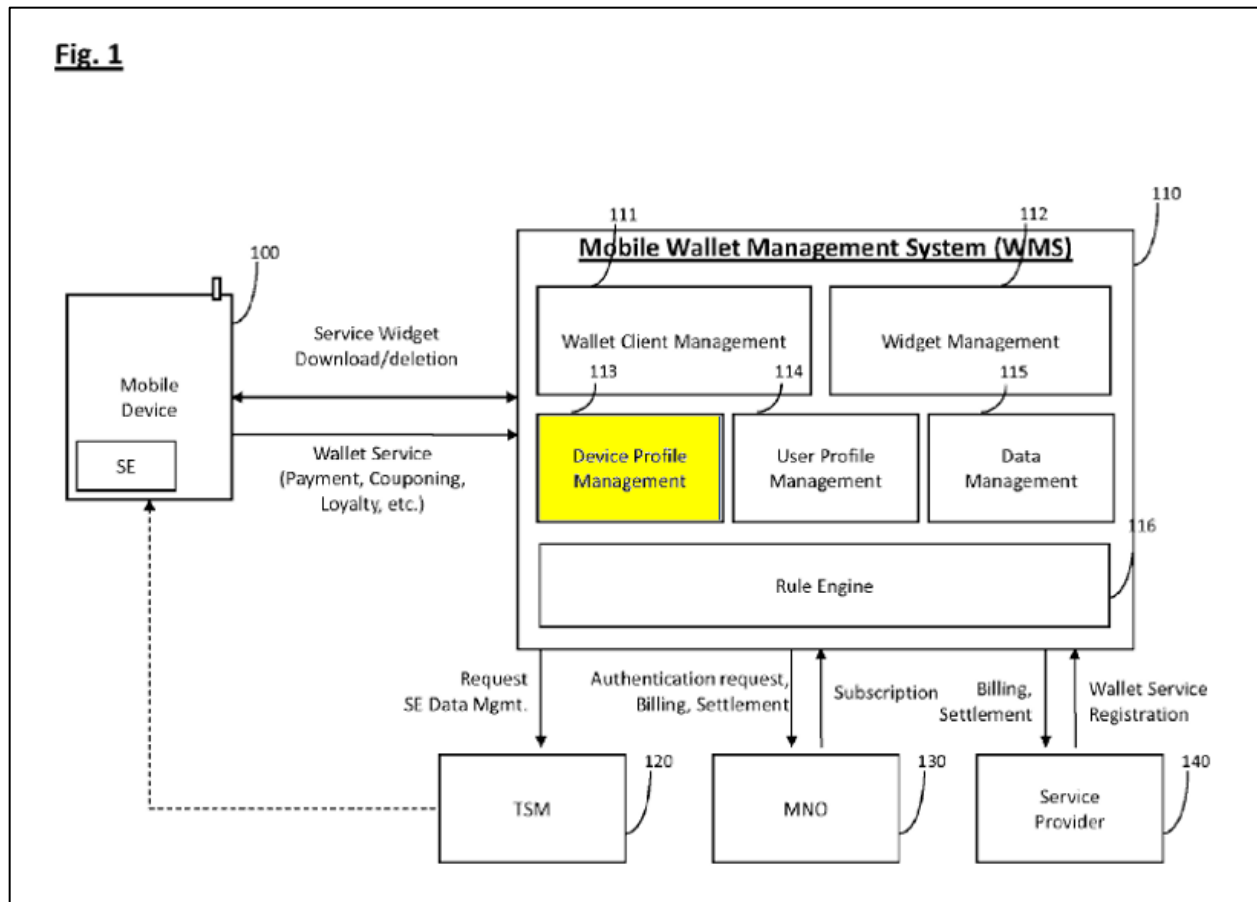
93. As I explained in the Summary of the ’125 Patent section above, the ’125 patent purports to have solved the problem of users being “bombarded with various applications that may be inapplicable to the user” due to differing mobile device hardware and software. ’125 patent, col. 2:30-44. The patent says this was a “limitation of current mobile wallet applications.” *Id.*, col. 2:30. And the patent’s proffered solution was for a server to filter for compatible mobile wallet applications based on mobile device information and offer only the compatible applications to the user. *See, e.g., id.*, col. 4:64-67; 5:12-16; and 10:45-55 (“As many mobile devices operate with various operating systems and standards, not all of the applets provided by the SP may be compatible with the user mobile device or user’s MNO. Because of lack of standardization of hardware and software on mobile devices, an efficient method to filter only the relevant applets

is helpful... [An] additional filtering mechanism may be provided to provide only the applicable applets to the requesting user.”).

94. In view of this, a POSITA would have understood that a mobile wallet application was capable of being independently downloaded and installed on a mobile device with an existing operating system. The ’853 provisional discusses the compatibility of various mobile platforms such as Android, Blackberry, Windows Mobile and Palm-Pre, each of which ran a different operating system. ’853 provisional, Business Requirements at page 6. And the ’125 patent explains that mobile wallet applications were available from different providers. *See, e.g.*, ’851 provisional, ¶84 (“Mobile wallet application 41, such as a SK C&C wallet”); ’125 patent, col. 4:64-67 (“mobile wallet application manufactured by Google®”); and ’851, Requirements Use Cases document at p. 41 (“The system shall check what type of wallet has been used (either SK C&C wallet or the third-party wallet.)”).

95. The patent explains that the “Device Profile management component 113” on the remote server “store[s] device specific information, such as information related to the mobile device itself including type of mobile device, supporting operating system (OS), mobile service provider, and other relevant information.” ’125 patent, col. 5:12-15; *see also id.*, col. 10:26-34 (referring to “mobile device 100 hardware specifications (i.e. hardware, software, operating system, etc.)”); *id.*, col. 10:45-47 (“As many mobile devices operate with various operating systems and standards, not all of the applets provided by the SP may be compatible with the user mobile device”); ’846 provisional, ¶30 (“Device Profile management component 203 may store device specific information, such as the apparatus itself including type of mobile device, supporting operating system (OS), and other relevant information.”); ¶64; ’851 provisional, ¶54 (“[T]here may be some technical limitations in providing certain products to user mobile equipment, such as incompatible mobile operating systems.”); ’853 provisional, ¶56 (referring to “incompatible mobile operating systems”). The stated reason that the device profile

management component stored information like the operating system version was to make “a filtered list of products...available for request by the consumer.” ’853 provisional, ¶56. The device profile management component is illustrated in Figure 1 of the patent on the server and highlighted in yellow in the reproduction of Figure 1 below:



96. Claim 18 itself says that the “wallet client management component [is] configured to store and to manage a mobile wallet application.” If the wallet was not a downloadable application that could be installed on a mobile device, there would be little, if any, need for a wallet client management component. Additionally, claim 1 is expressly directed to “[a] method for installing a wallet application in a mobile device,” which further informs the understanding of a POSITA that the ability of a mobile wallet application to be downloaded and installed on a

mobile device was part and parcel of what constituted a mobile wallet application in the '125 patent.

97. The understanding of a POSITA that mobile wallet applications are capable of being downloaded and installed is reinforced throughout the combined specification. For example, the download concept is reflected in the glossary of the '853 provisional, which says that a "Mobile Wallet" is "[a] downloadable mobile application for mobile commerce service in the user's handset." '853 provisional, Business Requirements, page 30. And the installation concept is conveyed in the '125 patent, which discloses "a method for installing a wallet application in a mobile device including requesting, by the mobile device, a mobile wallet application..., receiving mobile wallet application installation information; installing the mobile wallet application in the mobile device." '125 patent, col. 3:1-7. This makes it readily apparent to a POSITA that the operating system on the mobile device either does not already include any wallet management software or is superseded by the software specified in the '125, and that under either scenario it would be necessary to install wallet software as described. Fig. 2 of the '125 patent shows "[a] method for installing a mobile wallet application and associated management applet in a secure element (SE)." *Id.*, col. 5:47-49. "[T]he TSM system 120 will confirm the mobile wallet application installation request and initiate the wallet application installation process." *Id.*, col. 6:17-19. "TSM system 120 transmits the requested mobile wallet application 24 to mobile device 100 for installation." *Id.*, col. 6:34-36; *see also, e.g.*, '846 provisional, ¶33; '851 provisional, ¶26, ¶62 ("Ideally, once the mobile wallet application has been installed onto the mobile device, the customer will launch the mobile wallet application."); '853 provisional, ¶41 ("Once the requesting mobile device has installed a mobile wallet...").

98. In light this of these repeated and extensive disclosures, a POSITA would have understood that a "mobile wallet application" in the '125 patent was a mobile wallet software application capable of being independently downloaded and installed.

**D. “SE Information” (claims 14 and 23)**

99. As an initial matter, a POSITA in 2010 would have understood the acronym “SE” to refer to “secure element.” The claims and disclosure in the ’125 patent both make this clear. *See, e.g.*, ’125 patent, col. 1:38. The term “secure element” was itself a technical term of art in 2010. A POSITA at the time of the ’125 patent’s alleged priority date would have understood that the term “SE information” is also a technical term that, if read without context, could refer to two things: i) information about or relating to a secure element itself; or ii) information stored in the secure element. Although claim 14 (which says that SE information is “retriev[ed]”) and claim 23 (which says that SE information is “capture[d]”) provide little, if any, guidance as to what the SE information actually is, the specification does, as explained further below.

100. In view of the intrinsic record, a POSITA at the time of the ’125 patent’s alleged priority date would have understood that “SE information” is “information relating to the secure element.”

101. A POSITA would have come to this understanding based on the ’125 patent specification’s discussion of SE information as information relating to the secure element. For example, the ’125 patent lists at column 6:52-62 certain technical examples of SE information that relate to the specific SE in a particular device, all of which are information relating to the secure element (“SE information (e.g. Card Production Life Cycle (CPLC), Card Serial Number (CSN), Card Image Number (CIN), Integrated Circuit Card Identification (IC-CID))”). The “Requirements Use Cases” SK C&C product document that is incorporated by reference into the specification lists more general examples of SE information, which also all are information relating to the secure element but are not specific to a particular SE in a particular device, like the secure element’s “type,” operating system platform and version, and chip model and manufacturer. *See* ’851 provisional, Requirements Use Cases at page 15. The SK C&C “Business Requirements” document that is also incorporated into the specification also lists

comparable SE information, such as the SE type, logo, supported CCAs, platform, and status. *See* '853 provisional, Business Requirements document at pages 16-17.

102. A POSITA would not understand that “SE information” was limited to the specific examples enumerated in the specification. Rather, in my opinion, a POSITA would understand that SE information meant “information relating to the secure element” which captures the common thread that runs throughout the examples given in the '125 patent specification. A POSITA, however, would not have understood “SE information,” as that term is used and described in the '125 patent, to broadly include any possible type of information stored in the secure element and a construction that allowed for such inclusion would be contrary to the understanding of a POSITA.

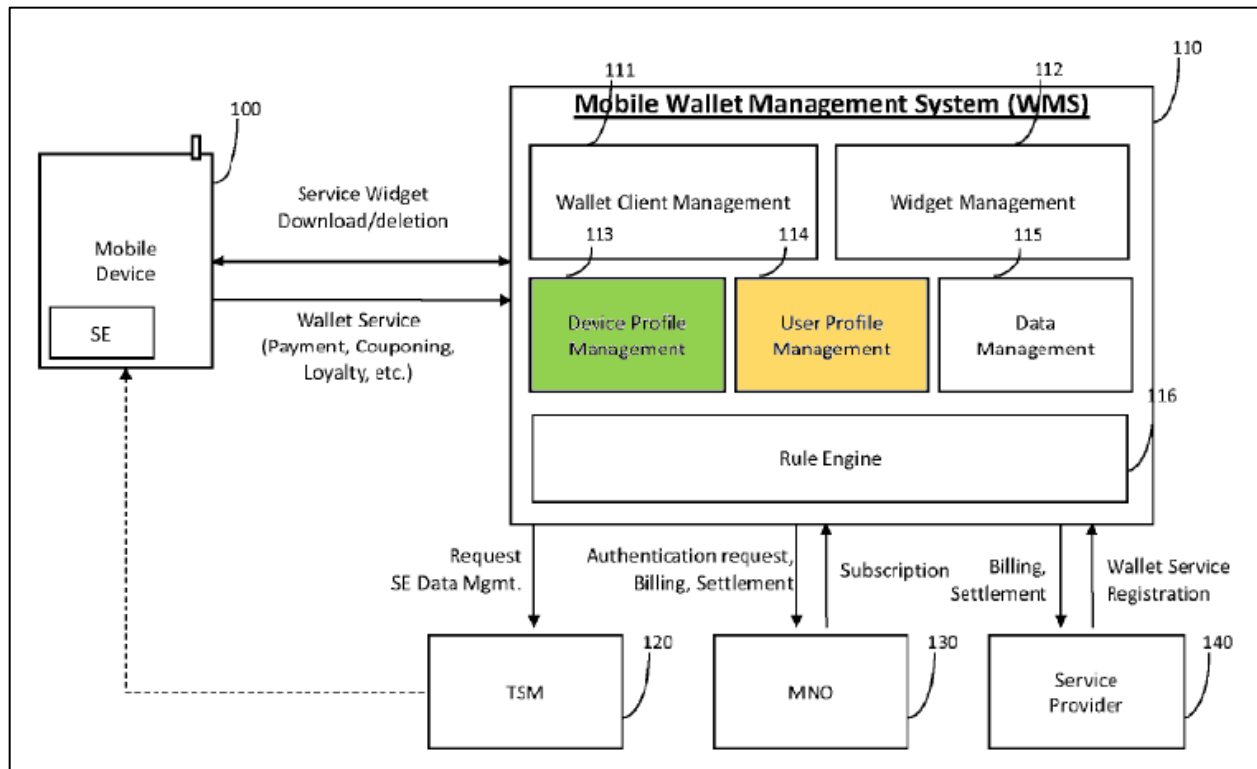
**E. “Mobile Device Information” (claims 14, 18, and 23)**

103. A POSITA at the time of the '125 patent's alleged priority date would have understood that the term “mobile device information,” when read as a complete phrase, is a technical term. In view of the intrinsic evidence, a POSITA at the time of the '125 patent's alleged priority date would have understood “mobile device information” to mean “hardware or software properties relating to the mobile device.”

104. A POSITA would have come to this understanding based on the '125 patent's repeated and consistent discussion of mobile device information as information relating to a hardware or software property of the mobile device. For example, claim 20 recites a list of exemplary mobile device hardware and software properties: “a mobile device type, a supporting Operating System (OS), a mobile service provider, a mobile device manufacturer, and a secure element (SE) type.” The '125 patent specification includes a similar list at column 5:9-16: information related to the mobile device itself including type of mobile device, Supporting operating system (OS), mobile service provider, and other relevant information.” Further, the specification also describes mobile device “hardware, software, operating system, etc.” as the mobile device's “attributes.”

'125 patent, col. 10:18-34. The fact that claim 23 states “mobile device information comprising SE information” is itself yet another example of this. Because the secure element is a part of the mobile device, information relating to the secure element’s hardware or software *is* information relating the mobile device’s hardware or software. In light these repeated descriptions, a POSITA would have understood that the mobile device information claimed in the '125 patent refers to hardware or software properties relating to the mobile device.

105. A POSITA would not have understood mobile device information to include user information, because user information is about the user and mobile device information is about hardware or software properties relating to the mobile device. A construction that included such additional information (e.g., user information) would be contrary to the understanding of a POSITA in view of the intrinsic evidence. A POSITA would understand that user information and mobile device information are distinct types of information. The '125 patent itself makes this clear. For instance, Figure 1 of the '125 patent shows different server components for storing mobile device information and user information. In particular, the device profile management component 113 (highlighted in green) stores mobile device information and is illustrated as being distinct and separate from the user profile management component 114 (highlighted in orange) which stores user information. *See* '125 patent, col. 5:12-22.



106. The specification explains that user profile management component 114 “captures user identifying information such as name, address, birthday, phone number, and the like” (’125 patent, col. 5:15-22) and that device profile management component 113 “store[s] device specific information, such as information related to the mobile device itself including type of mobile device, supporting operating system (OS), mobile service provider, and other relevant information” (*id.*, col. 5:9-16). *See also id.* at 10:26-34.

107. Claim 18 itself refers to a “device profile management component configured to store mobile device information,” but does not mention a user profile management component. Dependent claim 21, however, refers to “a user profile management component,” which reinforces the understanding of a POSITA that user information and mobile device information are different things. Claim 20 enumerates various types of mobile device information (“a mobile device type, a supporting Operating System (OS), a mobile service provider, a mobile device manufacturer, and a secure element (SE) type”), which are all hardware or software properties



relating to a mobile device. The '125 patent specification provides more examples of mobile device information, all of which relate to a hardware or software property of the mobile device. '125 patent, col. 5:9-16. Similarly, the specification describes various mobile device “attributes,” which include mobile device “hardware, software, operating system, etc.” *Id.*, col. 10:26-34. Although these are not expressly stated to be “mobile device information,” the patent’s discussion of using these “mobile device attributes” as part of the “filtering” process performed by the rule engine further confirms a POSITA’s understanding of what constitutes mobile device information. Based on these repeated characterizations and descriptions, a POSITA would understand “mobile device information” to mean hardware or software properties relating to the mobile device.

**F. “Over-the-Air (OTA) Proxy” (claim 23) and “OTA Proxy” (claim 16)**

108. The term “over-the-air (OTA) proxy” (or “OTA proxy” for short) was not a well-established term of art with a plain and ordinary meaning to a POSITA in 2010. Although a POSITA would likely have known that the acronym “OTA” stood for “over-the-air,” the broader phrase “OTA proxy” was just beginning to be used and had not achieved status as a term of art with a commonly understood meaning. To the extent the term “OTA proxy” was used in the 2010 timeframe, it was used sparingly and certainly did not have an established plain and ordinary meaning in the industry that would have been agreed upon by POSITAs.

109. As I mentioned in the paragraph above, OTA was a known acronym for “over-the-air.” In the context of a communication system involving mobile devices and servers, OTA generally referred to wireless transmissions between the mobile device and servers. For example, in a cellular communication system such as 3G or 4G LTE (which was just being introduced in the 2010 timeframe), OTA communications would take place over the mobile network (which could include a wireless connection like WiFi).

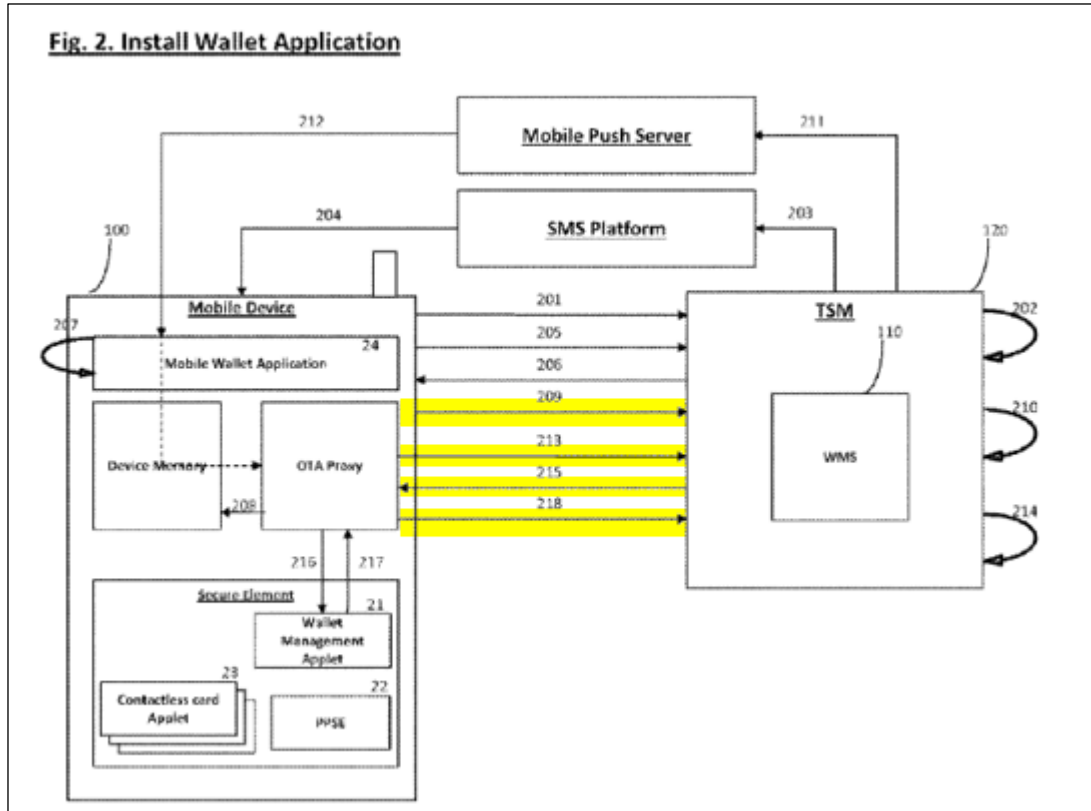
110. Separately, the term proxy or proxy server originally referred to an application running on piece of hardware (a server or router) used to manage data, (*e.g.*, “traffic”) commonly on a network, or in some cases on a specific device or subset of devices in a larger network. One of the first widely popular proxy server applications was the Apache Web server, which was developed in the Web era, in 1995. The Apache Web server may still be the most common proxy server in use today. Ex. K (Microsoft Computing Dictionary 2002, Fifth Edition). Due to the ubiquity of the Apache server proxy, a POSITA would understand a proxy server to have its functionality, namely accepting and managing requests using a set of rules for access and parameters for caching and performance shaping. Ex. L (“Apache the Definitive Guide 2nd edition,” Laurie, Ben and Laurie, Peter. 2000, O’Reilly & Associates, Sebastopol, CA). This is not a functionality that a POSITA would have expected to perform on a mobile device over-the-air in 2010.

111. Especially in view of the usage of the term “proxy” described above, a POSITA would not have understood what an OTA proxy was without seeing how that term was described and used in the ’125 patent.

112. A POSITA would, however, have understood the term “OTA proxy” upon reviewing the intrinsic evidence, which uses the term several hundred times. A POSITA reading the ’125 patent specification, including the provisional applications, would understand the term “OTA proxy” to mean a mobile device software application for communicating between a secure element and a server over a mobile network.

113. Consistent with a POSITA’s understanding of the term “OTA” described above, the ’851 provisional includes a glossary, which states that “Over-The-Air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile handset or any component within the mobile handset via the mobile network.” ’851, Requirements Use Cases at p. 55. OTA communications are also shown in Figures 2 and 3 of the ’125 patent and the

accompanying discussion. For instance, the '125 patent explains that the communications labelled 209, 213, 215, and 218 in Figure 2 (reproduced below with highlights on those steps) are OTA communications. *See* '125 patent, col. 6:63-64 (for step 209), col. 7:58-61 (for step 213), col. 8:2-4 (for step 215), and col. 8:15-17 (for step 218).



114. The patent specification consistently refers to the OTA proxy as a software application. For example, the '125 patent states that “TSM system 120 transmits the requested mobile wallet application 24 to mobile device 100 for installation and an accompanying over-the-air (OTA) proxy program to allow OTA provisioning in step 206.” '125 patent, col. 6:34-37; *see also id.*, col. 6:42-43 (“Once the mobile wallet application 24 and accompanying OTA proxy program have been downloaded, the mobile wallet application 24 may be launched”). A POSITA would understand the word “program” to be a reference to a software application.

115. Claim 23 states that the “OTA proxy is configured to capture mobile device information comprising SE [secure element] information,” indicating that the OTA communicates with the secure element. And the ’125 patent specification explains that “[o]nce TSM system 120 receives the information sent by OTA Proxy in step 213, TSM system 120 processes the information and converts the identifying information along with the request to provision WMA 21 container into Application Protocol Data Unit (APDU) commands in step 214 and sends them over to OTA proxy in step 215. Next, in step 216, OTA proxy receives the APDU commands to install WMA 21 container and relays them to the SE, which processes the APDU commands to install the requested WMA 21 container and its associated credentials. SE then responds back with the result of each command request in step 217.” ’125 patent, col. 7:66-8:10; *see also, e.g., id.*, col. 9:14-19 (““Once TSM system 120 receives the information sent by OTA Proxy, TSM system 120 processes the received information along with the provisioning command and converts both the received information along with the provisioning command into APDU commands to send to OTA proxy in step 309.”). In view of these descriptions, and similar disclosures throughout the combined specification, a POSITA would understand that the role of the OTA proxy was to communicate between the secure element and TSM server, acting as an interface between them.

116. The ’851 provisional discusses the OTA proxy extensively. *See*, ’853, ¶27 (“A more detailed explanation on the OTA proxy may be found in the co-pending [’851] provisional application.”). The “Summary” of the ’851 provisional begins by stating that “OTA proxy is a mobile client which supports OTA post-issuance related services to the secure element in a mobile communication device.” ¶10. A POSITA would understand the “mobile client” to be a software program. The ’851 provisional explains that it “provide[s] a system to install OTA Proxy application onto the mobile device.” ¶¶14-15. A POSITA would understand this to mean that the OTA proxy is a software application that must be installed on the mobile device. The

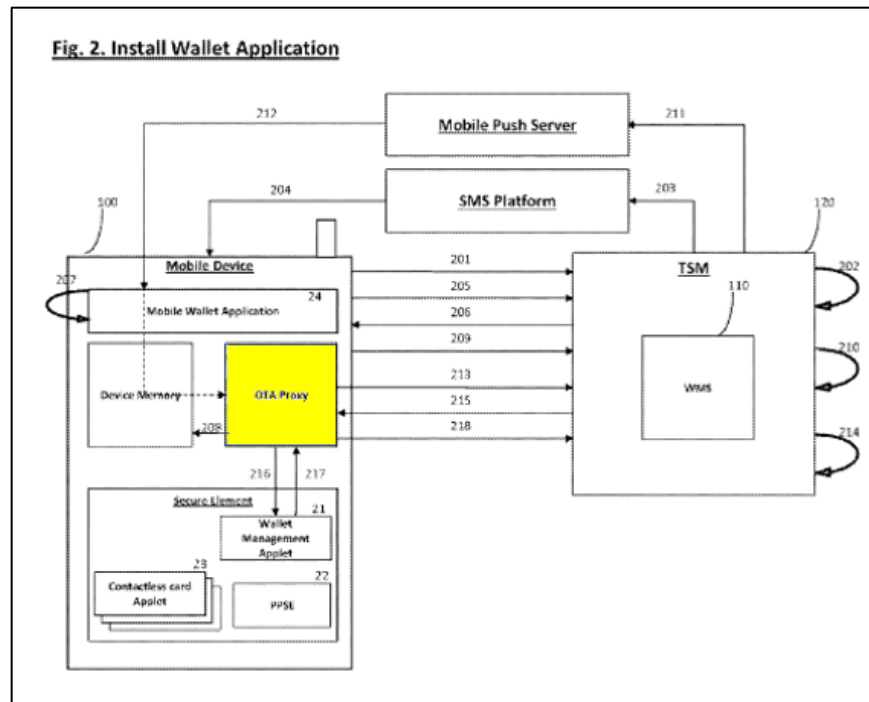
'851 provisional goes on to again refer to "OTA Proxy application 42 software." ¶58, 83. The '853 provisional says that "[t]he OTA proxy shall be a stand-alone application or a subcomponent of a wallet application," again confirming that is a software program. '853, Business Requirements document at pp. 4-5.

117. It was commonplace in 2010 to install one piece of software into another, such as by providing a software update or patch that is installed into an existing software application, like a Microsoft Office software update. Software patching was a common practice as early as the 1960's, when IBM used system software patches (installed by hand by a system operator on reel-to-reel tape) to update system and application functionality on the fly (or with a few system restarts). In fact, the idea of the software patch was so common, and commonly taught in programming curriculum, that the aforementioned Apache proxy server got its name because it was considered "a patchy" system. Even more popularly, as early as the Windows 95 operating system in 1995, Microsoft used what became called the Windows Update application to manage operating system updates. These updates were implemented so that the updater application would check the device's hardware and software attributes, and if an operating system or application update was available, notify the user and provide them with an easy graphical user interface to perform the update. By this time, the ubiquity of updates, even to everyday computer users, not just a POSITA, was well known. Many applications, such as Microsoft's own Office applications, had their own update functionality. For example, in Microsoft Word, a user could add or update Word functionality by installing or updating Macros or add-ins to provide additional functionality like more elaborate toolbar interfaces or macros to customize format and print party invitations. These updates could be done manually or by using a graphical interface, usually a simple menu selection followed by a few selections in a pop-up dialog box. These updates often didn't require that the device or even the application be restarted.

118. The fact that the OTA proxy “may be included in the mobile wallet application” (’125 patent, col. 6:61-62) or is described a “subcomponent” of a wallet application (’853 provisional at pages 4-5) doesn’t mean that the OTA proxy isn’t a software application. For all the reasons explained above, it was well understood in 2010 that one application could be installed into another, and a POSITA would have understood that the OTA proxy was a software application.

119. The ’853 provisional further explains that “OTA proxy 42 is a necessary component to the present disclosure which is necessary to provision confidential information, such as financial applications and related account information into the mobile device's SE. The OTA Proxy is a mobile client which supports OTA post-issuance related services to the secure element in a mobile communicative s device. As SE types, Micro SD and Embedded SEs cannot support conventional SAT/SUSAT/CAT framework, OTA Proxy over OTA is necessary for any party to send data to mobile communicative devices with the specified memory types.” ¶77. A POSITA would understand this passage to mean exactly what it says—that the OTA proxy is “necessary” to the purported invention to “provision confidential information to the [secure element].” The OTA proxy was necessary, the patent explains, to accommodate a variety of types of different secure elements, including “non-UICC SE types, such as Micro SD and Embedded SE.” *Id.*; see also ’851, ¶10 (“OTA Proxy over OTA may be used by any party to send data to mobile communicative devices with the non-UICC SE types, such as Micro SD and Embedded SE. However, if desired, OTA proxy can also provide an alternative method to provision OTA, over the conventional method, to SE devices which do support conventional SAT/SUSAT/CAT framework.”). These disclosures, again, affirm that the OTA proxy communicates between a secure element and server, such as a provisioning TSM server.

120. This is even illustrated in the figures, which show the OTA proxy installed on the mobile device in communication with the secure element (and TSM server). Figure 2 is reproduced below with the OTA proxy highlighted in yellow.




121. Further technical details about communicating with various types of secure elements are discussed in various places throughout the specification. *See, e.g.*, '851 provisional, ¶¶72-86; '853 provisional, Business Requirements at pp. 12-13.

122. In summary, it is my opinion is that a POSITA would understand the term “OTA Proxy” in the '125 patent to be mobile device software application for communicating between a secure element and a server over a mobile network.

**G. “Provision[ing]” (claims 11 and 23)**

123. I was not asked to render an opinion on the term “provision[ing].”

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 3<sup>rd</sup> day of October, 2019 in Vancouver, BC.

  
Don Turnbull, PhD